**CLAIMS:**

1. (Currently amended) A method for authenticating a message, comprising:

performing a security function upon the message to generate a message authentication code, wherein the security function utilizes at least one publicly known constant to perform the security function upon the message, and wherein the at least one publicly known constant is selected from a set of publicly known constants used to implement the security function;

sending the message to a receiver;

sending the ~~output of the security function to a target~~ message authentication code to the receiver; and

sending the at least one publicly known constant, used by the security function to perform the security function upon the message, to the receiver[[;]], wherein the receiver authenticates the message based on the message authentication code and the at least one publicly known constant ~~authenticating the received message as a function of at least a shared key, the received publicly known constants, the security function, the received message, and the output of the security function~~.

2. (Original) The method of Claim 1, wherein the security function comprises a hash function.

3. (Currently amended) The method of Claim 1, wherein the authentication comprises a determination that the message is at least one of authentic or not authentic.

4. (Canceled).

5. (Currently amended) The method of Claim 1, wherein the security function further comprises at least one of an encryption function or a decryption function.

6. (Canceled)

7. (Currently amended) A system for authenticating messages, comprising:

a source node having a shared key, security logic and a set of publicly known constants required to implement the security logic on messages transmitted by the source node; and

a target node also having the shared key and the security logic, the target node further configured to receive at least one selected publicly known ~~constants~~ constant from the source node, but not storing the set of publicly known constants, wherein the source node transmits a message, a message authentication code, and at least one selected publicly known constant selected from the set of publicly known constants, to the target node and the target node authenticates the transmitted message based on the message authentication code and the at least one selected publicly known constant.

8. (Original) The system of Claim 7, wherein the source node comprises a computer.

9. (Original) The system of Claim 7, wherein the security logic is configured to implement a hashing function.

10. (Original) The system of Claim 7, further comprising an unsecured medium coupled between an output of the source node and an input of the target node.

11. (Currently amended) The system of Claim 7, wherein the source node is further configured to generate a message authentication code (MAC) as a hash of at least the message, the at least one publicly known constant, and a secret key.

12-14. (Canceled)

15. (Currently amended) A computer program product for authenticating a message, the computer program product having a medium with a computer program embodied ~~thereon, the computer program comprising~~:

computer code for performing a security function upon the message to generate a message authentication code, wherein the security function utilizes at least one publicly known constant to perform the security function upon the message, and wherein the at least one publicly known constant is selected from a set of publicly known constants used to implement the security function;

computer code for sending the message to a target;

computer code for sending the ~~output of the security function to a target~~ message authentication code to the target; and

computer code for sending the at least one publicly known constant, used by the security function to perform the security function upon the message, to the target[[; and]], wherein the receiver authenticates the message based on the message authentication code and the at least one publicly known constant ~~computer code for authenticating the received message as a function of at least a shared key, the received publicly known constants, the security function, and the received message~~.

16. (Currently amended) A processor for authenticating a message, the processor including a computer program comprising:

computer code for performing a security function upon the message to generate a message authentication code, wherein the security function utilizes at least one publicly known constant to perform the security function upon the message, and wherein the at least one publicly known constant is selected from a set of publicly known constants used to implement the security function;

computer code for sending the message to a target;

computer code for sending the ~~output of the security function to a target~~ message authentication code to the target; and

computer code for sending the at least one publicly known constant, used by the security function to perform the security function upon the message, to the target[[; and]], wherein the receiver authenticates the message based on the message authentication code and the at least one publicly known constant ~~computer code for authenticating the received message as a function of at least a shared key, the received publicly known constants, the security function, and the received message~~.

17. (New) The method of Claim 1, wherein the security function is a Secure Hash Algorithm (SHA), and wherein the set of publicly known constants comprises the first 64 bits of the fractional parts of the cube roots of the first eighty prime numbers.

18. (New) The method of Claim 1, wherein the receiver does not store the set of publicly known constants.

19. (New) The method of Claim 1, further comprising:

authenticating, at the receiver, the message as a function of at least a shared key, the at least one publicly known constant, the security function, the message, and the message authentication code.

20. (New) The method of Claim 1, further comprising:

computing, at the receiver, a second media access code based on the received at least one publicly known constant, the received message, and a secret key stored by the receiver;

comparing the second media access code to the received media access code; and

determining that the received message is authentic in response to the second media access code matching the received media access code.

21. (New) The method of Claim 2, wherein the hash function is applied to a secret key, the at least one publicly known constant, and the message such that the resulting message authentication code is equal to a hash of the combination of the secret key, the at least one publicly known constant, and the message.

22. (New) The system of Claim 7, wherein the security function is a Secure Hash Algorithm (SHA), and wherein the set of publicly known constants comprises the first 64 bits of the fractional parts of the cube roots of the first eighty prime numbers.

23. (New) The system of Claim 7, wherein the target node authenticates the message as a function of at least a shared key, the at least one publicly known constant, the security function, the message, and the message authentication code.

24. (New) The system of Claim 7, wherein the target node:

computes a second media access code based on the received at least one publicly known constant, the received message, and a secret key stored by the receiver;

compares the second media access code to the received media access code; and

determines that the received message is authentic in response to the second media access code matching the received media access code.

25. (New) The system of Claim 9, wherein the hashing function is applied to a secret key, the at least one publicly known constant, and the message such that the resulting message authentication code is equal to a hash of the combination of the secret key, the at least one publicly known constant, and the message.